第一章　畢氏三元組

定義. 滿足不定方程 $x^2+y^2=z^2$ 的正整數 x,y,z 稱爲**畢氏三元組**。若 $\gcd(x,y,z)=1$, 我們稱其爲**基本解** [3]。

引理 1. 若 x,y,z 是一組畢氏三元組, 則 $\gcd(x,y)=\gcd(x,z)=\gcd(y,z)$。

證明. 因爲

$$\gcd(y,z)^2=\gcd(y^2,z^2)=\gcd(y^2,x^2+y^2)=\gcd(y^2,x^2)=\gcd(y,x)^2,$$

我們有 $\gcd(y,z)=\gcd(y,x)$。同樣地,

$$\gcd(x,z)^2=\gcd(x^2,z^2)=\gcd(x^2,x^2+y^2)=\gcd(x^2,y^2)=\gcd(x,y)^2,$$

所以 $\gcd(x,z)=\gcd(x,y)$, 得證。 $\square$

引理 2. 若 x,y,z 是不定方程 $x^2+y^2=z^2$ 的基本解, 則 x,y,z 兩兩互質且 x,y 爲一奇一偶。

證明. 根據引理 1, $\gcd(x,y)=\gcd(x,z)=\gcd(y,z)$, 所以我們只須證明 $\gcd(x,y)=1$ 即可。若 $\gcd(x,y)>1$, 則存在一個質數 p 使得 $p\mid x$ 且 $p\mid y$, 因此 $p\mid x^2+y^2=z^2$, 即 $p\mid z$。也就是說, p 是 x,y,z 的公因數, 這與 $\gcd(x,y,z)=1$ 矛盾, 所以 $\gcd(x,y)=1$。

另外, x,y 不能同爲偶數, 否則 $2\mid\gcd(x,y)$; 若 x,y 同爲奇數, 則 x,y 分別爲 $2x_1+1$ 和 $2y_1+1$ 的型式, 其中 $x_1,y_1\in\mathbb{Z}$。我們得到

$$x^2+y^2=4({x_1}^2+x_1+{y_1}^2+y_1)+2=z^2 \text{ 是偶數} \Rightarrow z \text{ 是偶數。}$$

令 $z=2z_1$, $z_1\in\mathbb{Z}$, 則 $z^2=4{z_1}^2$ 不是被 4 除餘 2, 矛盾。所以 x,y 必爲一奇一偶。 $\square$

我們想要求 $x^2+y^2=z^2$ 的一切基本解, 不失一般性, 可設 x 爲偶數。

定理 1. 不定方程 $x^2+y^2=z^2$ 的一切基本解皆爲以下的型式:

$$x=2ab,\quad y=a^2-b^2,\quad z=a^2+b^2, \tag{1}$$

其中

$$a>b>0,\quad \gcd(a,b)=1,\quad 2\nmid(a+b)\text{。}$$

證明. 先證由 (1) 式給出的 x, y, z 是不定方程的基本解 [5]。

$$x^2+y^2=(2ab)^2+(a^2-b^2)^2=a^4+2a^2b^2+b^4=(a^2+b^2)^2=z^2,$$

此外, 因爲 $\gcd(a,b)=1$,

$$\begin{aligned}\gcd(y,z)&=\gcd(a^2-b^2,a^2+b^2)\\&=\gcd(2a^2,a^2+b^2)\\&=\gcd(a^2,a^2+b^2)\\&=\gcd(a^2,b^2)\\&=\gcd(a,b)^2\\&=1,\end{aligned}$$

所以 $\gcd(x,y,z)=\gcd(x,\gcd(y,z))=\gcd(x,1)=1$。

再證不定方程的所有基本解都可以表示成式 (1) 的型式。因爲 $\gcd(x,y)=1$ 且 $2\mid x$, 故 y, z 都是奇數。此外, 由方程式 $x^2+y^2=z^2$ 可知

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2}。$$

我們證明 $\gcd(\frac{z+y}{2},\frac{z-y}{2})=1$。若 $\gcd(\frac{z+y}{2},\frac{z-y}{2})=d>1$, 則 $d\mid(\frac{z+y}{2}+\frac{z-y}{2})=z$ 且 $d\mid(\frac{z+y}{2}-\frac{z-y}{2})=y$, 所以 $d\mid\gcd(y,z)=1$, 矛盾。因此 $\gcd(\frac{z+y}{2},\frac{z-y}{2})=1$。因爲 $(\frac{x}{2})^2$ 是完全平方數且 $\gcd(\frac{z+y}{2},\frac{z-y}{2})=1$, 所以 $\frac{z+y}{2}$ 和 $\frac{z-y}{2}$ 皆是完全平方數。我們可設 $\frac{z+y}{2}=a^2$, $\frac{z-y}{2}=b^2$, $a>b>0$, 我們得到 $x=2ab$, $y=a^2-b^2$, $z=a^2+b^2$。另外, 因

$$1=\gcd\left(\frac{z+y}{2},\frac{z-y}{2}\right)=\gcd(a^2,b^2)=\gcd(a,b)^2,$$

故 $\gcd(a,b)=1$。最後, 因爲 y 是奇數且 $y=a^2-b^2$, 代表 a, b 必須是一奇一偶, 換句話說 $2\nmid(a+b)$。 □

事實上, 不定方程 $x^2+y^2=z^2$ 的一切正整數解皆型如

$$x=2kab,\quad y=k(a^2-b^2),\quad z=k(a^2+b^2), \tag{2}$$

其中 $k\in\mathbb{N}$, a, b 的條件同定理 1。我們現在要證明每一組基本解都唯一對應一組互質的 (a,b)。若有兩組互質的 (a_1,b_1) 與 (a_2,b_2) 對應同一組基本解, 我們有

$$\begin{cases}2a_1b_1=2a_2b_2 & \cdots\cdots\cdots ①\\ {a_1}^2-{b_1}^2={a_2}^2-{b_2}^2 & \cdots\cdots\cdots ②\\ {a_1}^2+{b_1}^2={a_2}^2+{b_2}^2 & \cdots\cdots\cdots ③\end{cases},$$

將 ③ 加減 ① 得

$$\begin{cases} ③+①: \ (a_1+b_1)^2=(a_2+b_2)^2 \\ ③-①: \ (a_1-b_1)^2=(a_2-b_2)^2 \end{cases}$$
$$\Rightarrow \begin{cases} a_1+b_1=a_2+b_2 \\ a_1-b_1=a_2-b_2 \end{cases}$$
$$\Rightarrow \begin{cases} a_1=a_2 \\ b_1=b_2 \end{cases}。$$

此外, 不定方程 $x^2+y^2=z^2$ 的每一組正整數解亦唯一對應一組 (k,a,b)。

情形一: 若存在 (k_1,a_1,b_1) 和 (k_2,a_2,b_2) 使得

$$\begin{cases} k_1(2a_1b_1)=k_2(2a_2b_2) & \cdots\cdots\cdots④ \\ k_1({a_1}^2-{b_1}^2)=k_2({a_2}^2-{b_2}^2) & \cdots\cdots\cdots⑤ \\ k_1({a_1}^2+{b_1}^2)=k_2({a_2}^2+{b_2}^2) & \cdots\cdots\cdots⑥ \end{cases},$$

則我們將 ⑥ 加減 ⑤ 得到

$$\begin{cases} ⑥+⑤: \ k_1(2{a_1}^2)=k_2(2{a_2}^2) & \cdots\cdots\cdots⑦ \\ ⑥-⑤: \ k_1(2{b_1}^2)=k_2(2{b_2}^2) & \cdots\cdots\cdots⑧ \end{cases}$$

$$\Rightarrow \frac{⑦}{⑧}: \ \left(\frac{a_1}{b_1}\right)^2=\left(\frac{a_2}{b_2}\right)^2。$$

因爲 $\frac{a_1}{b_1}$ 及 $\frac{a_2}{b_2}$ 皆爲正, 所以

$$\frac{a_1}{b_1}=\frac{a_2}{b_2}。$$

此外, $\gcd(a_1,b_1)=1=\gcd(a_2,b_2)$, 因此 $a_1=a_2$, $b_1=b_2$。代回 ④, 我們得 $k_1=k_2$。

情形二: 若存在 (k_1,a_1,b_1) 和 (k_2,a_2,b_2) 使得

$$\begin{cases} k_1(2a_1b_1)=k_2({a_2}^2-{b_2}^2) & \cdots\cdots\cdots⑨ \\ k_1({a_1}^2-{b_1}^2)=k_2(2a_2b_2) & \cdots\cdots\cdots⑩ \\ k_1({a_1}^2+{b_1}^2)=k_2({a_2}^2+{b_2}^2) & \cdots\cdots\cdots⑪ \end{cases},$$

則我們將 ⑨ 除以 ⑩:

$$\frac{⑨}{⑩}: \frac{2a_1b_1}{{a_1}^2-{b_1}^2}=\frac{{a_2}^2-{b_2}^2}{2a_2b_2} \qquad \cdots\cdots\cdots⑫,$$

再將 ⑫ 乘以 $2a_2b_2({a_1}^2-{b_1}^2)$, 我們得到 $4a_1a_2b_1b_2=({a_1}^2-{b_1}^2)({a_2}^2-{b_2}^2)$。因爲等號左邊爲偶數, 但右邊卻是奇數, 矛盾, 所以情形二不會成立。

是否對每個正整數 n, 一定能找到直角的一邊爲 n 的畢氏三元組? 現在要證明 $n\geq 3$ 是一定有的。

引理 3. 對每一個正整數 $n\geq 3$ 皆存在以 n 爲直角的一邊的畢氏三元組。

證明. 當 n 爲奇數, 取 $x=\dfrac{n^2-1}{2}$, $z=\dfrac{n^2+1}{2}$, 則

$$x^2+n^2=\left(\frac{n^2-1}{2}\right)^2+n^2=\left(\frac{n^2+1}{2}\right)^2=z^2。$$

當 n 爲偶數, 取另一邊爲 $\dfrac{n^2}{4}-1$, z 爲 $\dfrac{n^2}{4}+1$, 則

$$n^2+\left(\frac{n^2}{4}-1\right)^2=\left(\frac{n^2}{4}+1\right)^2=z^2。$$

□

當 $n=1$ 或 2 時是找不到的。若 $n=1$, 則 n 爲 (2) 式中 y 的型式 (因爲 $2kab$ 是偶數, n 不會是 x 的型式), 所以

$$n=k(a^2-b^2)=k(a-b)(a+b)=1。$$

因 k 與 $a-b$ 皆爲正, 故 $k=a-b=a+b=1$, 計算 a,b 得到 $a=1,b=0$, 與 $b>0$ 矛盾, 所以不存在直角的一邊爲 1 的畢氏三元組。若 $n=2$, 情形一: $n=2kab$。則 $k=a=b=1$, 與 $a>b$ 矛盾。情形二: $n=k(a^2-b^2)$。則 (k,a,b) 所有的可能爲

$$① \ (2,1,0),\ ② \left(1,\frac{3}{2},-\frac{1}{2}\right),\ ③ \left(1,\frac{3}{2},\frac{1}{2}\right)。$$

① 與 $b>0$ 矛盾, ②、③ 與 $a,b\in\mathbb{N}$ 矛盾, 所以不存在直角的一邊爲 2 的畢氏三元組。